PayDirect Overview

FIS presents our comprehensive Web, Point-of-Sale (POS) and Interactive Voice Response (IVR) solutions for accepting various payments electronically. By partnering with FIS, clients are able to contract with a single vendor for all needs related to electronic payments, providing a single source of accountability for services provided. The flexibility of our solution allows clients to utilize any or all payment applications. It is your choice. Additionally, payment types and methods are flexible and can be configured to meet the unique needs of each department or transaction type. Further, new departments, payment types, and payment methods can be quickly added providing a solution that will carry you well into the future. The payment solution is fully hosted by FIS and integrates into our PCI DSS Level I compliant payment gateway for payment processing, ensuring high reliability and security at all times. Our solution includes:

- Access to our PCI DSS compliant Internet payment gateway for real-time payment processing and reporting
- An easy-to-use Application Programming Interface (API) for existing application/software integration
- Intuitive, customizable Web payment applications
- Convenient, user-friendly Point-of-Sale (POS) and Virtual terminals
- A fully functional, multi-lingual Interactive Voice Response (IVR) system
- Processing of all types of electronic payments (credit, debit, e-check)
- A single source for settlement of all payment types through all payment channels
- An online reporting tool with information on all transactions and settlements in real time
- Full training and support services, including Project and Relationship Management personnel
- Multiple Merchant IDs (MIDs) supported

Internet Payment Gateway

The electronic payment solution FIS deploys for a client will integrate into our fully-hosted Internet payment gateway for payment processing and real-time reporting. Our gateway provides comprehensive functionality and exceptional security and dependability. It is fully PCI DSS compliant, and has further security credentials via our Independent Validation and Verification (IV&V) certification granted through the U.S. Treasury Department. The high level of availability provided by our gateway is accomplished through a sophisticated array of redundant systems and protocols.

Our gateway connects directly into the nation's largest payment processors allowing clients to accept an array of payment methods. It is fully capable of processing credit, signature debit, PIN debit, PINless debit, and smart cards. It processes all major credit cards (Visa, MasterCard, American Express, and Discover). Our gateway can also process all major debit networks. In fact, FIS owns and operates NYCE, one of the country's largest debit networks. In addition, FIS' gateway accepts payments via e-check/ACH.

One of the unique facets of FIS' gateway is its ability to accept and track up to six (6) client-defined fields of data, known as "user parts", along with a payment transaction. In addition to the standard fields of data FIS tracks per transaction, user parts enable clients to store additional data inside each individual transaction. This data is made available through our online reporting tool, as well as the merchant activity file that is available to clients. By utilizing user parts, clients can customize the information contained in each transaction. User parts have a length of up to 255 characters and may include data such as citizen account numbers, street address, registration number, etc.

Additional attributes of our gateway include, but are not limited to:

- Full compliance with Visa, MasterCard, American Express, and Discover
- Real-time authorizations

- PCI certified
- IV&V Certification for U.S. Treasury Dept.
- Supports multiple payment channels and methods
- Split settlement capabilities
- Consolidated settlement capabilities
- Seamless integration with the Client’s existing website(s)
- Duplicate and fraudulent payment prevention
- Automatic convenience fee calculation
- Real-time, customizable payment reporting services via the Internet

Web Application

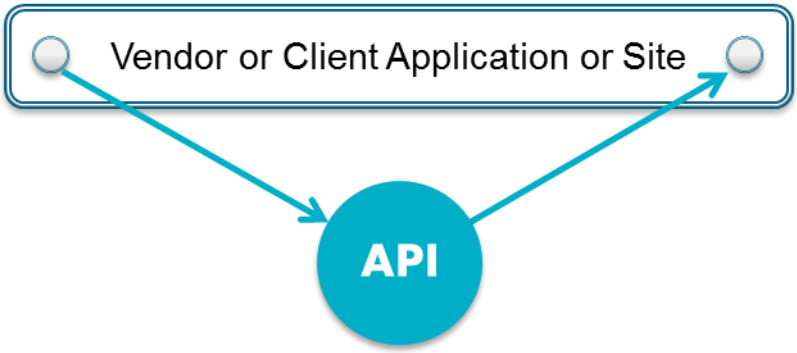
Application Programming Interface (API) Payment Flow

Note: FIS' API is typically used when a client uses an internal or vendor hosted payment solution that is already PCI certified and they want to use the FIS gateway to authorize transactions.

FIS' Application Programming Interface (API) offers a quick and easy way for clients to integrate existing software packages, applications, and systems with our payment gateway. The procedures necessary for developing to our gateway are detailed in our Web Payment Gateway (API) Specifications document, which may be provided upon request. By following these specifications, a client or your third party development firm(s) may interface existing applications or software with our payment gateway for payment processing and real-time reporting.

Once a transaction is initiated via the API, data is sent to FIS' gateway through an HTTPS post. Once the post is received, the data is transmitted to the backend processor. A response is then received back from the processor and our database is updated. Return data is then sent to the client.

Transactions occur in real-time, with responses sent back to the client within seconds. This immediate response enables the client to immediately post payment data to your information system, providing a record of the results of the transaction.



Key Features Include:

- Can accept payments directly within an existing business application client's or your vendor's)
- TLS Encryption
- Simple certification process
- Speed to market controlled by the client
- Variety of payment methods
- Variety of acquirers through a single interface
- Convenience Fee capable
- Visa Program capability built-in

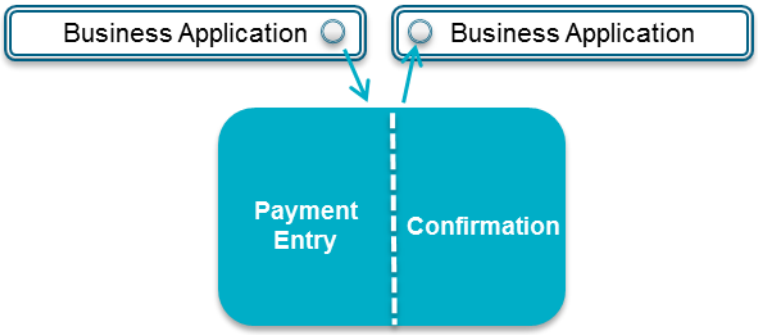
Note: The following payment flows are typically used when a client seamlessly routes the customer to the FIS hosted solutions where sensitive account data is collected and authorizations occur. How much the client wishes to host on their front end website will determine which payment flow best applies.

Pass-Through Payment Flow

FIS' Pass-Through Payment Flow allows clients to validate customers and present billing information on your existing website and then link customers to our secure website for the actual entry of sensitive payment information. This application works by providing a payment site that seamlessly integrates with the client's existing website(s), eliminating the need for the client to handle, transmit, or otherwise "touch" sensitive payment information.

The client will present billing information then pass the customer over to FIS to handle the sensitive payment information. Through a POST to FIS by the client, the balance of the customer's account will be passed through to the payment pages designed and maintained by FIS. User-entered payment amounts are also available based upon the client's preference. Once the payment is processed, the customer will be passed back to the client for completion of the transaction process, including receipt presentation. FIS will pass information indicating the status of the transaction back to the client's website via a post-back method for the receipt. This will also allow real-time updates to the client's system.

FIS will build Payment Entry and Payment Confirmation pages that look and feel just like the pages on the client's existing website, providing a seamless experience for your customers.



Key Features Include:

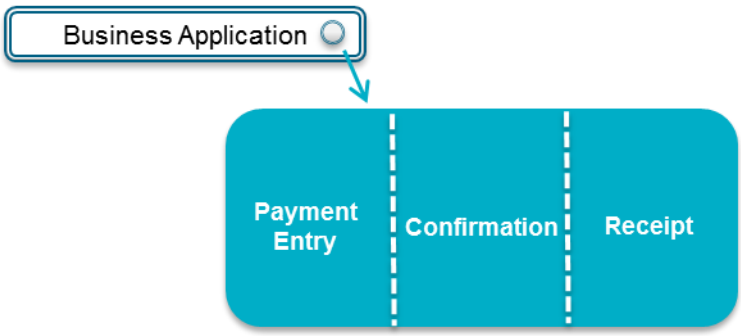
- Can leverage an existing business application (the client's or your vendor's) while offloading a majority of the PCI burden to FIS
- TLS Encryption
- Rapid implementation on the standard application
- Variety of payment methods and acquirers
- Convenience Fee capable
- Visa Program capability built-in
- Look and feel is configured to remain consistent with the client's branding

In-Flight Payment Flow

Like the Pass-Through, FIS' In-Flight Payment Flow allows the client to validate customers and present billing information on your existing website and then link customers to our secure website for the actual entry of sensitive payment information. This payment flow works by providing a payment site that seamlessly integrates with the client's existing website(s), eliminating the need for the client to handle, transmit, or otherwise "touch" sensitive payment information. The client validates customers through your

systems, while payment information is collected by FIS. Through a POST to FIS by the client, the balance of the customer's account is passed through to the payment pages designed and maintained by FIS. User-entered payment amounts are also available based upon the client's preference. Once the payment is processed, FIS presents the receipt and the transaction is complete.

FIS will build Payment Entry, Payment Confirmation, and Receipt pages that look and feel just like the pages on the client's existing website, allowing customers to make payments confidently and securely.



Key Features Include:

- Can leverage an existing business application (the client's or your vendor's) while offloading a majority of the PCI burden to FIS
- TLS Encryption
- Rapid implementation on the standard application
- Variety of payment methods and acquirers
- Convenience Fee capable
- Visa Program capability built-in
- Look and feel is configured to remain consistent with the client's branding

Non-Validating Payment Flow

FIS' Non-Validating Payment Flow provides a payment site, accessible through a unique URL that allows a customer to choose their own payment obligation. We then collect all payment information. FIS will build Data Entry, Payment Entry, Payment Confirmation, and Receipt pages, creating a customer-friendly, easy-to-use payment portal.

Key Features Include:

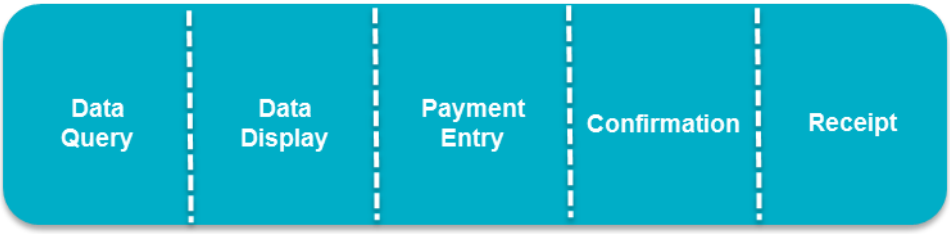
- No billing information specific to the user is presented.
- The customer selects from standard options presented and pays for what they have chosen.
- FIS handles all sensitive payment information and presents the receipt.
- Intended where no business application exists on the client's side, and where there is simple criteria desired for making a payment

- Rapid implementation on the standard application
- Variety of payment methods and acquirers
- Convenience Fee capable
- Visa Program capability built-in
- Look and feel is configured to remain consistent with the client's branding

Validating Payment Flow

FIS' Validating Payment Flow provides a payment site, accessible through a unique URL, with account validation and bill summary presentment capabilities. This payment flow allows customer account validation and the collection of payment details for all types of payments. Through an end user load file that is provided by the client, FIS is able to validate user information and present proper billing details. The customer is then required to enter a shared secret, PIN, invoice number, or other identifier to retrieve their account information. We then collect all payment information, process the payment, and present the receipt.

FIS will build Data Query, Data Display, Payment Entry, Payment Confirmation, and Receipt pages, creating a customer-friendly, easy-to-use payment portal.

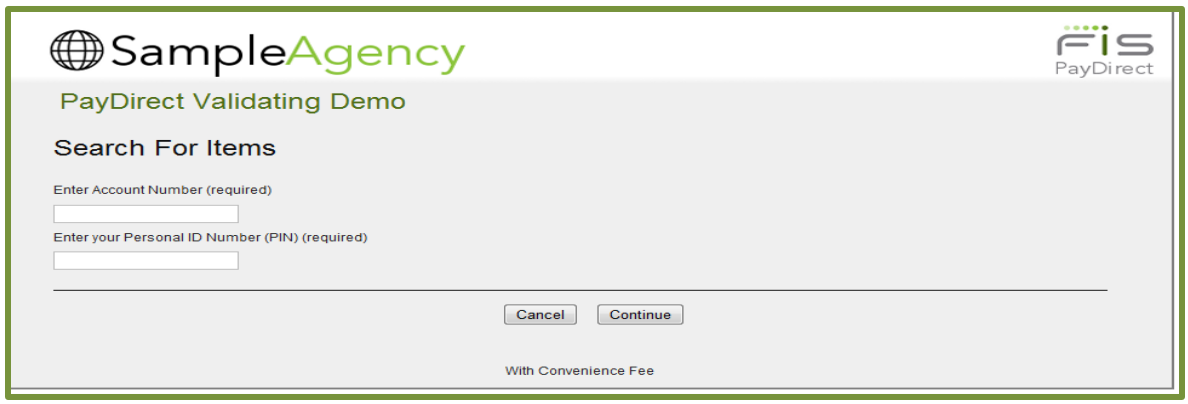


Key Features Include:

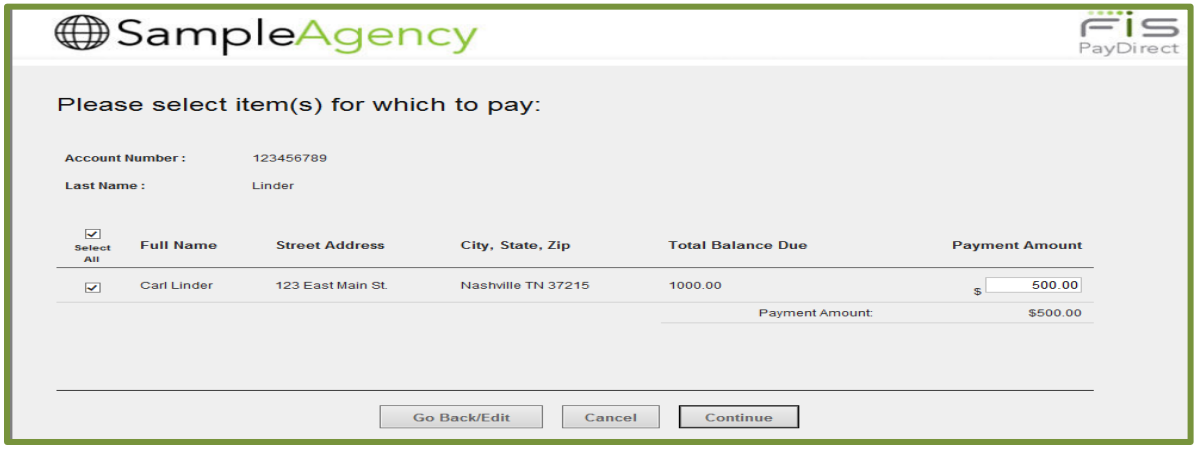
- Intended where no business application exists on the client's side, but where there is data that is used to validate a user and what they are paying for.
- Rapid implementation on the standard application
- Variety of Payment Methods and Acquirers
- Convenience Fee capable
- Visa Program capability built-in
- Look and Feel is configured to remain consistent with the client's branding

Following are sample screenshots from FIS' Web Application. NOTE: Validating Model Payment Flow represented.

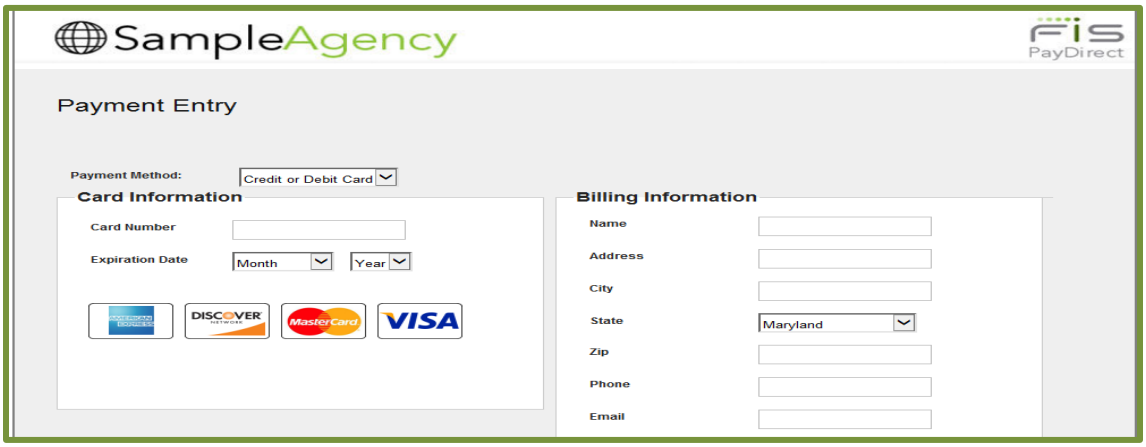
Data Query Page



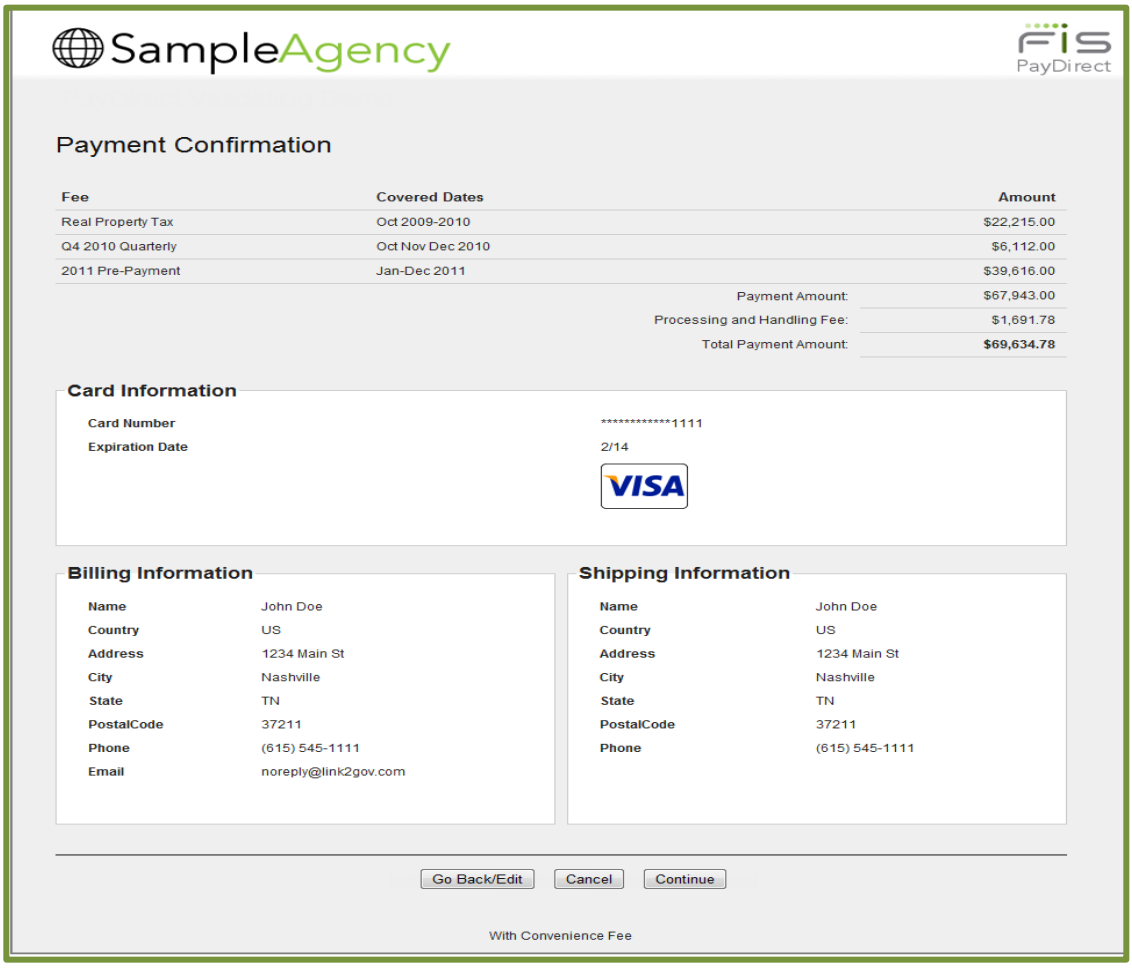
Data Entry Page



Payment Entry Page



Payment Confirmation Page



Receipt Page

Point-of-Sale

FIS offers and supports a convenient line of Point-of-Sale (POS) solutions that enables the client's employees to perform an immediate, real-time authorization of a customer's account during face-to-face transactions. Our POS solutions also enable the processing of mailed-in payments, as well as payments taken in a call center environment. We can install point-of-sale terminals or a Web-based virtual terminal solution to meet your POS payment processing needs.

Point-of-Sale Devices

FIS deploys and supports the VeriFone Vx series terminals (or comparable models) for accepting face-to-face credit and debit payments. These terminals allow the option to process payments through a dial-up connection, Wi-Fi, Ethernet, or cellular. They have a small counter-top footprint and are an all-in-one terminal, printer, and PINpad.

PIN Entry Devices

The client's departments processing debit transactions may incorporate a VeriFone VX805 external PINpad (or comparable model). These devices offer a compact design that is perfect for customer-entered PIN numbers at the sales counter.

Check Reader Devices

For those departments interested in accepting checks at the Point-of-Sale, we offer the MagTek MiniMICR check reader (or comparable model). This device connects directly to the VeriFone terminals, making check-based payments just as convenient as credit and debit.

MultiPay

FIS utilizes our own MultiPay application for use with the point-of-sale terminals. This application has the following features:

- Custom, government centric POS application
- Supports multiple receipts – one for the customer and one for the client
- Sales, voids, & refunds
- Key-entered, Swipe, Swipe & PIN
- Accepts Signature debit, PIN debit, Visa, MC, Amex, Discover, & e-Check
- Dial, IP, Cellular, or Wi-Fi
- Additional PINpad may be tethered to main terminal device
- Check MICR reader may be tethered to main terminal device
- Convenience Fee capable
- Host-based transaction batching
- Employs shopping cart functionality for multiple payments
- Supports up to 20 custom payment items
- Enables customer reference number tracking
- Transaction reporting at a user/terminal level
- Split Settlement Capable
- Enables "Payment Items" tracking
- Employs user authentication with access privileges
- Supports customer-defined disclaimer on receipts

- Duplicate payment sensitivity
- Utilizes TLS encryption
- Supports multiple users on the same device
- Receipt Barcode for transaction data capture
- Quick Flow version for Retail environment

Virtual Terminal

FIS offers our exclusive Virtual Terminal as a browser-based terminal solution for the client. This solution allows the client to use your existing computers as POS terminals that communicate through the Internet to process a variety of payments. Virtual Terminal is perfect for transactions occurring at the point-of-sale, processing mailed-in credit card payments, or for call centers accepting payments via live operators.

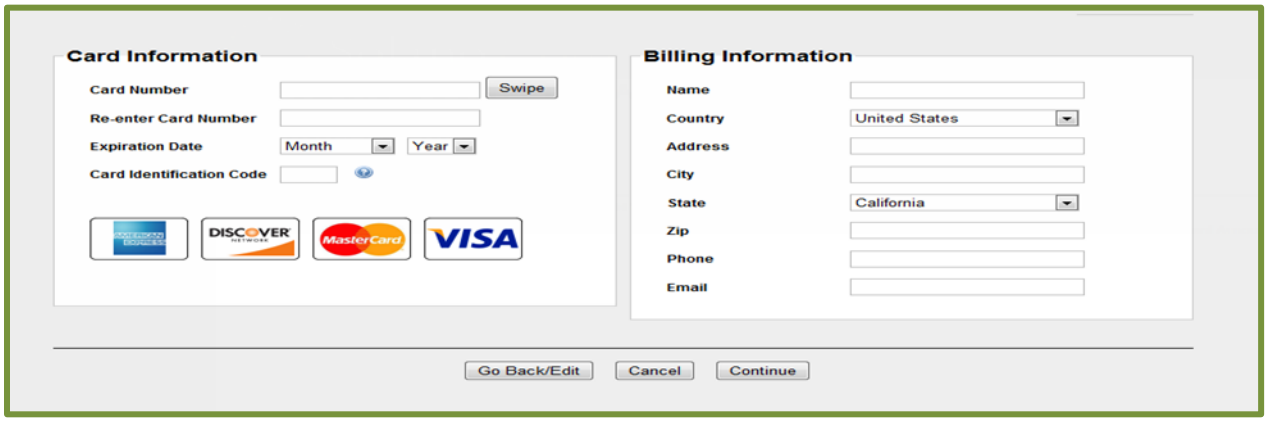
Key Features Include:

- Browser-based payment application
- Fast, scalable setup and integration
- No additional peripherals required
- Sales, voids and refunds
- Accepts Signature debit, Visa, MC, Amex, Discover
- Convenience Fee capable
- Multiple line item settlement
- Call center or back-office environment: Key-entered
- Over the Counter environment: Key-entered, Swipe supported
- Host-based transaction batching
- Enables customer reference number tracking
- Duplicate payment sensitivity
- Automated system stays current with the most up-to-date release
- Visa Program compliant

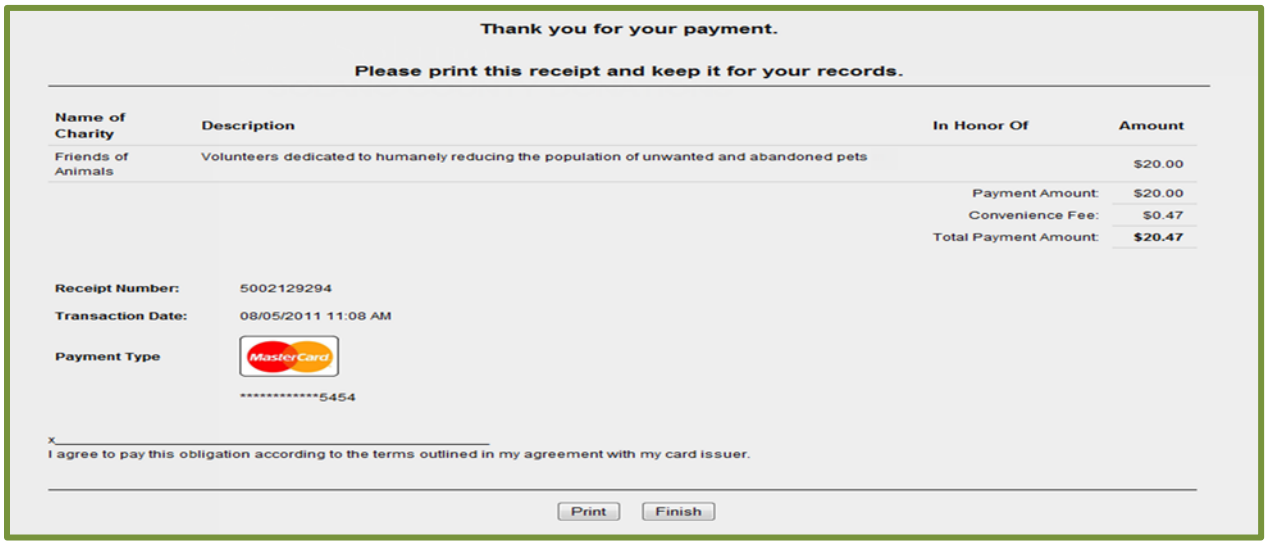
The following are sample screenshots from the Virtual Terminal.

Swipe Payment Entry Screen

Manual Payment Entry Screen



Receipt Page with Signature Line



Interactive Voice Response (IVR)

FIS' IVR has been simplified to provide a faster turnaround from implementation activities to the production environment. This is accomplished by having a flexible predefined call flow and configurable prompt variables to customize the caller experience to the business need for the telephone payment channel.

Speed to market is not the only benefit to the new model. Studies show a 20% increase in simplicity results in a 96% increase in customer loyalty. With a noticeable portion of your payments handled over the phone, a simple IVR that makes it easy for callers has a huge payoff.

Some of the features include:

- Multiple languages, including English and Spanish

- Multiple payment methods
- Convenience Fee capable
- Requires acceptance of convenience fee prior to processing of payment
- Opt-out/cancel option prior to processing of payment
- Split settle capable
- Utilizes professional, accent neutral voice talent
- Communications with third-party software applications, and open APIs
- Key-ahead prompting
- IVR transfers

By offering multiple channels of communication including voice, Web, etc., customers can be served based on their preferred method of communication. An example is the choice of an immediate email confirmation of a voice-enabled transaction. Database driven applications may also be performed, such as offering customer-specific menus based on their unique account type or status. The IVR can also consume Web services for customer verification and updates.

Configurable Business Verbiage within IVR Select Prompts

The IVR provides configurable prompt variables that allows the business to choose what the caller hears within select call flow prompts, including:

- Client Name
- Client Website Address
- Client Phone Number
- Liability Name
- Preamble of Service to the Caller
- Card Descriptor

DataPointe Client Console

FIS provides advanced, real-time transactional reporting via our DataPointe Client Console. Authorized client employees are able to generate transaction, batch, and refund reports to verify and manage transaction history. The Reporting application is versatile in report creation and presentation, permitting users to omit displayed fields and save frequently generated reports. Reports may be grouped and sorted as well. In addition to the reporting features, refunds can be submitted and tracked online.

Key features include:

- Transaction history review
- Customized reconciliation reports
- Transaction, monthly, refund, line item, and batch summary reports
- Transaction activity tracking by agency
- Convenience fee reporting
- Credit card, debit card, and check volume analysis
- Ad-hoc queries using the search tool
- Browse transaction level detail
- View new retrieval requests daily
- Export data to XML, CSV, TIFF, PDF, and Excel

There are a considerable number of configurable reports available within DataPointe. These reports have a large number of filter options, layout options, and other configurations giving users extensive flexibility in configuring reports to meet their specific needs. All reports are available 24/7. Transaction data is available for a period of 3 years (a rolling 36 months) through the online reporting application. Reports available include:

- Transactions – Transaction details
- Transaction Summary – Summary of transaction detail
- Batch – Batch details for a single batch id
- Batch Detail – Summarized information by Batch (status)
- Batch Summary – Summarized information by Batch (financial)
- Line Item – Line item details
- Line Item Summary – Summary of Line item detail
- Refund – Refunds by transaction id
- Monthly – Monthly transaction totals by payment method
- User Report – Provided upon request
- Merchant Comparison – Comparison of volume for merchant(s) for 2 time periods
- Invoice Summary – Summary level batch information
- eCheck Return – eCheck return information
- ACH AV Reconciliation – Shows ACH AV transaction attempts

Merchant Activity File

In addition to the online reporting, FIS generates a daily, custom Merchant Activity File (MAF) in a flat file format that may be retrieved via our secure FTP site. Produced at the close of business each day, this file allows the client to reconcile transactions and update systems with payment information. The Merchant Activity File is created three to four hours after settlement cut time and includes transaction data that is generated from settlement batches. The data fields available within the merchant activity file are all data components associated within a transaction. This file will contain data for all successful transactions from the previous day.

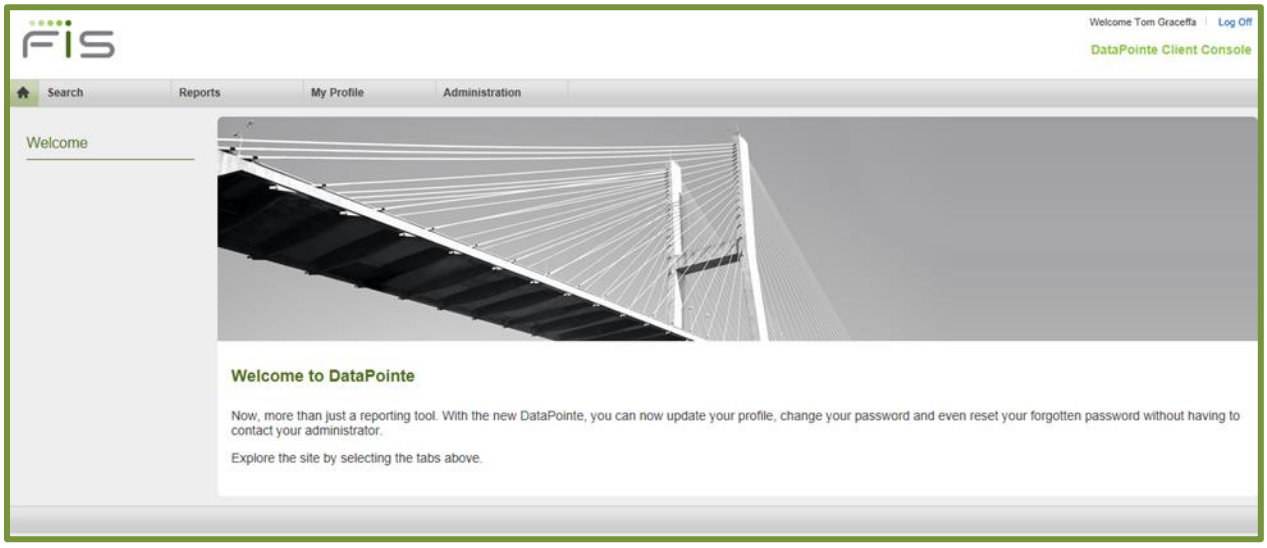
During the implementation process, FIS will collaborate with client personnel to develop a custom Merchant Activity File layout based on your individual specifications. Below are sample fields that may be included in the file.

Transaction ID	Time Stamp	Merchant Time Stamp
L2G Merchant Account	Payment Type	Transaction $ Amount
Convenience $ Fee	Merchant's $ Amount	Card/Check Last 4
Card/Check Extra Data	User Part 1	User Part 2
User Part 3	User Part 4	User Part 5
User Part 6	Account/Billing Full Name	Account/Billing Address
Account/Billing City	Account/Billing State	Account/Billing Zip
Account/Billing Email	Account/Billing Phone	Authorization Code

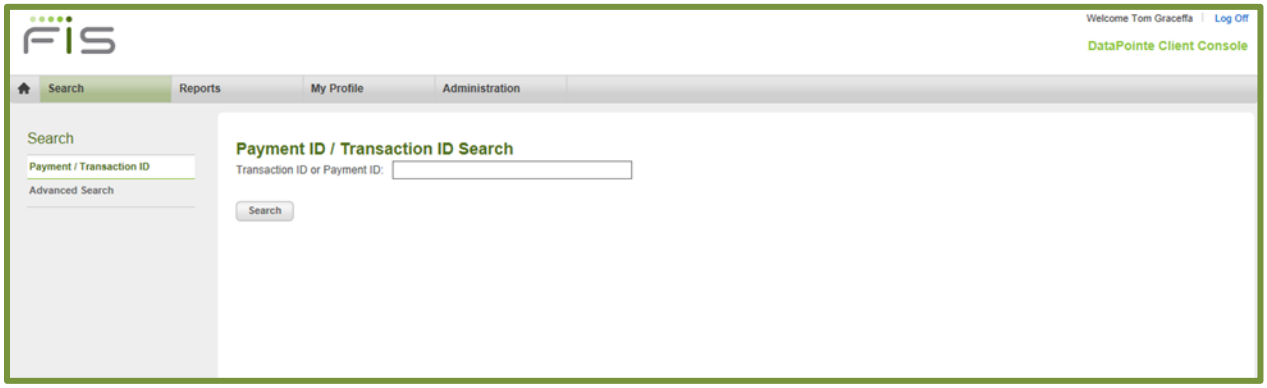
Following are screenshots from the DataPointe Client Console.

Login Page

Home Page

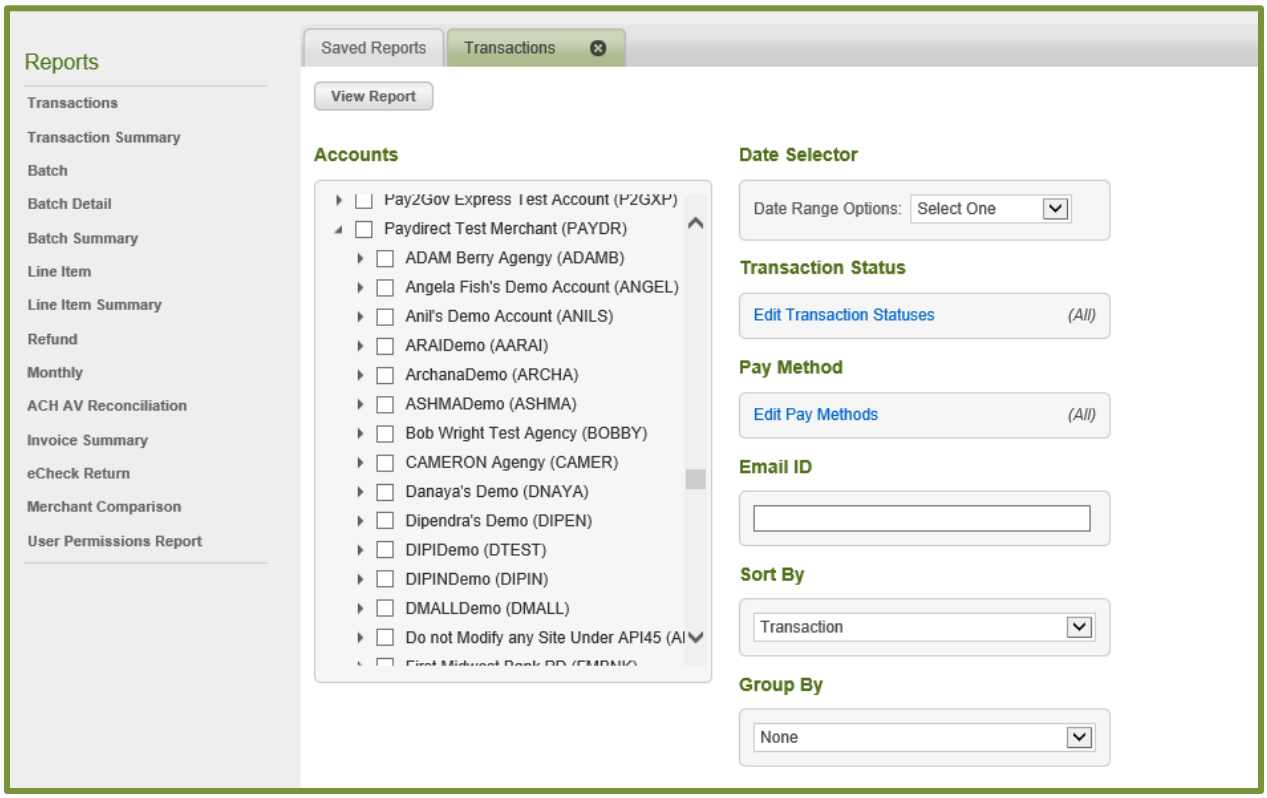


Search Page

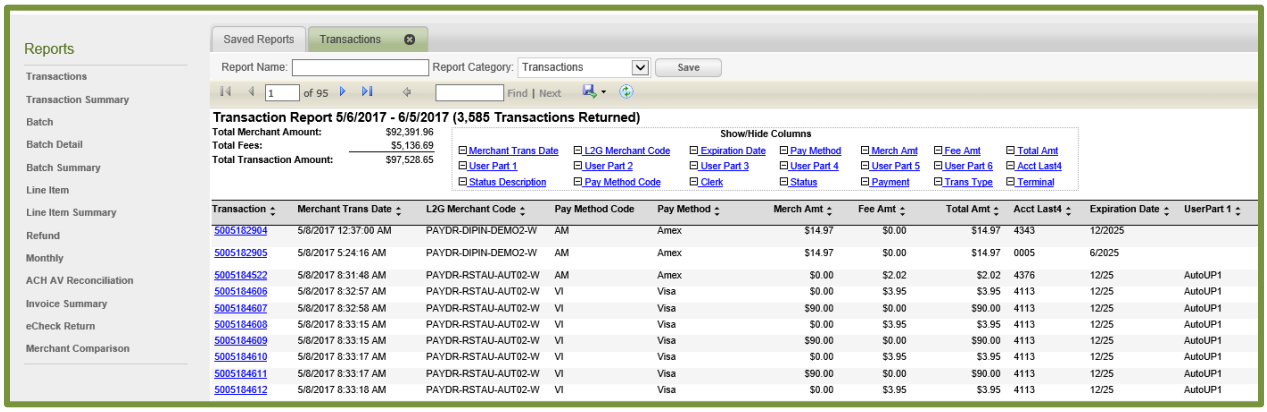


Saved Reports Page

Transaction Search Page



Sample Transactions Report



Reports

Transactions
Transaction Summary
Batch
Batch Detail
Batch Summary
Line Item
Line Item Summary
Refund
Monthly
ACH AV Reconciliation
Invoice Summary
eCheck Return
Merchant Comparison

Saved Reports | Transactions

Report Name: | Report Category: Transactions | Save

1 of 95 | Find | Next

Transaction Report 5/6/2017 - 6/5/2017 (3,585 Transactions Returned)

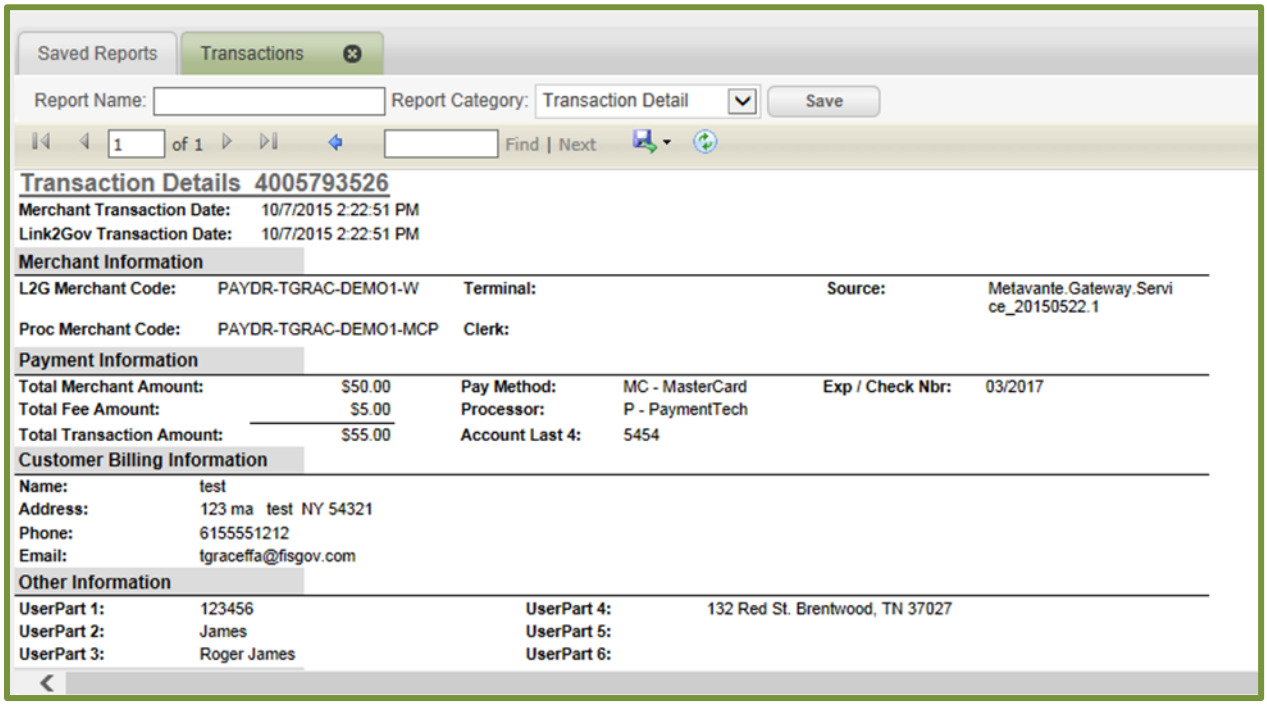
Total Merchant Amount:	$92,391.96
Total Fees:	$5,136.69
Total Transaction Amount:	$97,528.65

Show/Hide Columns

Merchant Trans Date | L2G Merchant Code | Expiration Date | Pay Method | Merch Amt | Fee Amt | Total Amt
User Part 1 | User Part 2 | User Part 3 | User Part 4 | User Part 5 | User Part 6 | Acct Last4
Status Description | Pay Method Code | Clerk | Status | Payment | Trans Type | Terminal

Transaction	Merchant Trans Date	L2G Merchant Code	Pay Method Code	Pay Method	Merch Amt	Fee Amt	Total Amt	Acct Last4	Expiration Date	UserPart 1
5005182904	5/8/2017 12:37:00 AM	PAYDR-DIPIN-DEMO2-W	AM	Amex	$14.97	$0.00	$14.97	4343	12/2025	
5005182905	5/8/2017 5:24:16 AM	PAYDR-DIPIN-DEMO2-W	AM	Amex	$14.97	$0.00	$14.97	0005	6/2025	
5005184522	5/8/2017 8:31:48 AM	PAYDR-RSTAU-AUT02-W	AM	Amex	$0.00	$2.02	$2.02	4376	12/25	AutoUP1
5005184606	5/8/2017 8:32:57 AM	PAYDR-RSTAU-AUT02-W	VI	Visa	$0.00	$3.95	$3.95	4113	12/25	AutoUP1
5005184607	5/8/2017 8:32:58 AM	PAYDR-RSTAU-AUT02-W	VI	Visa	$90.00	$0.00	$90.00	4113	12/25	AutoUP1
5005184608	5/8/2017 8:33:15 AM	PAYDR-RSTAU-AUT02-W	VI	Visa	$0.00	$3.95	$3.95	4113	12/25	AutoUP1
5005184609	5/8/2017 8:33:15 AM	PAYDR-RSTAU-AUT02-W	VI	Visa	$90.00	$0.00	$90.00	4113	12/25	AutoUP1
5005184610	5/8/2017 8:33:17 AM	PAYDR-RSTAU-AUT02-W	VI	Visa	$0.00	$3.95	$3.95	4113	12/25	AutoUP1
5005184611	5/8/2017 8:33:17 AM	PAYDR-RSTAU-AUT02-W	VI	Visa	$90.00	$0.00	$90.00	4113	12/25	AutoUP1
5005184612	5/8/2017 8:33:18 AM	PAYDR-RSTAU-AUT02-W	VI	Visa	$0.00	$3.95	$3.95	4113	12/25	AutoUP1

Sample Transaction Details Report:



Saved Reports | Transactions

Report Name: | Report Category: Transaction Detail | Save

1 of 1 | Find | Next

Transaction Details 4005793526

Merchant Transaction Date: 10/7/2015 2:22:51 PM
Link2Gov Transaction Date: 10/7/2015 2:22:51 PM

Merchant Information

L2G Merchant Code:	PAYDR-TGRAC-DEMO1-W	Terminal:		Source:	Metavante.Gateway.Service_20150522.1
Proc Merchant Code:	PAYDR-TGRAC-DEMO1-MCP	Clerk:			

Payment Information

Total Merchant Amount:	$50.00	Pay Method:	MC - MasterCard	Exp / Check Nbr:	03/2017
Total Fee Amount:	$5.00	Processor:	P - PaymentTech		
Total Transaction Amount:	$55.00	Account Last 4:	5454		

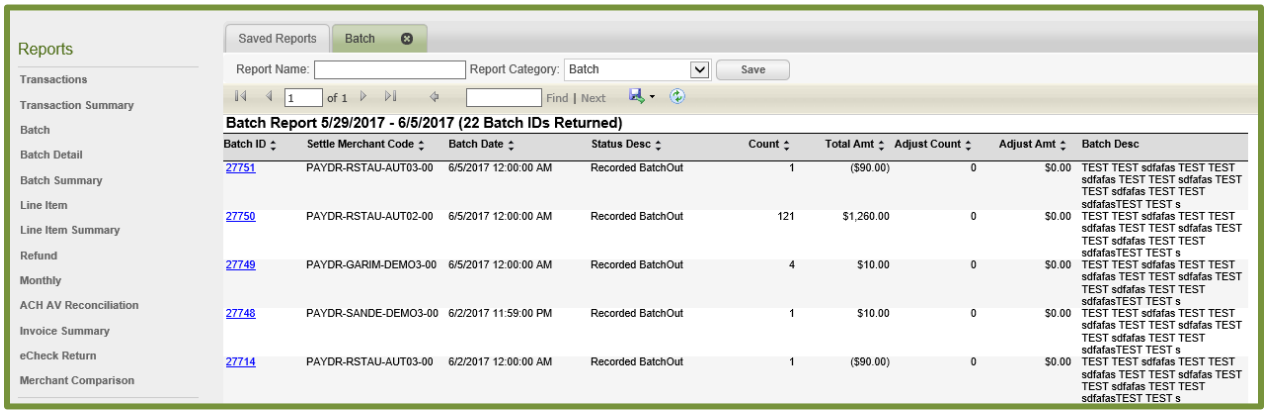
Customer Billing Information

Name:	test
Address:	123 ma test NY 54321
Phone:	6155551212
Email:	tgraceffa@fisgov.com

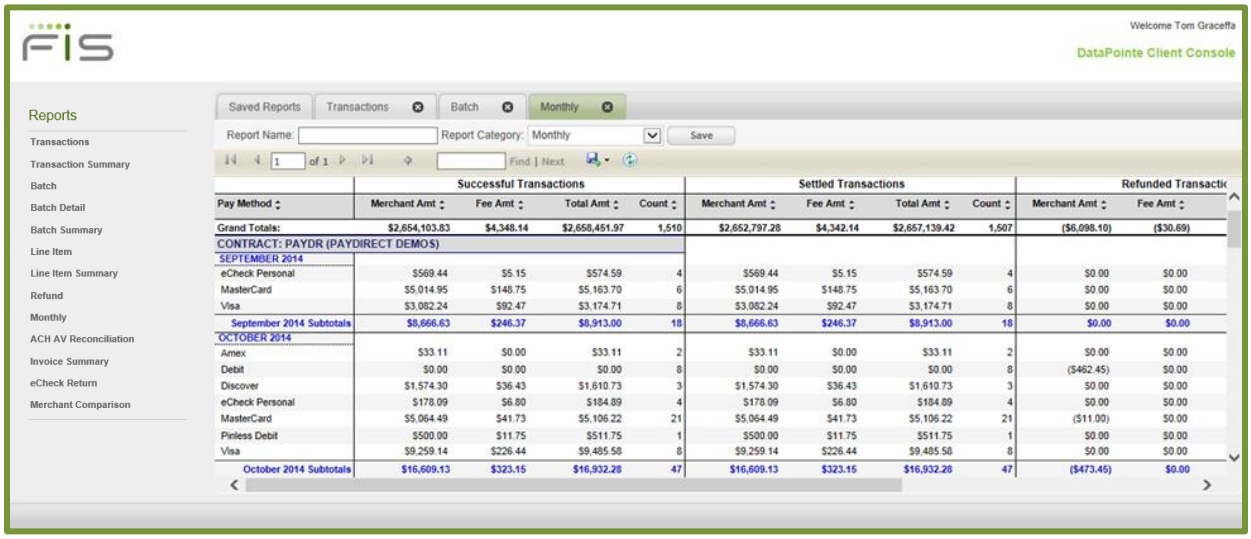
Other Information

UserPart 1:	123456	UserPart 4:	132 Red St. Brentwood, TN 37027
UserPart 2:	James	UserPart 5:	
UserPart 3:	Roger James	UserPart 6:	

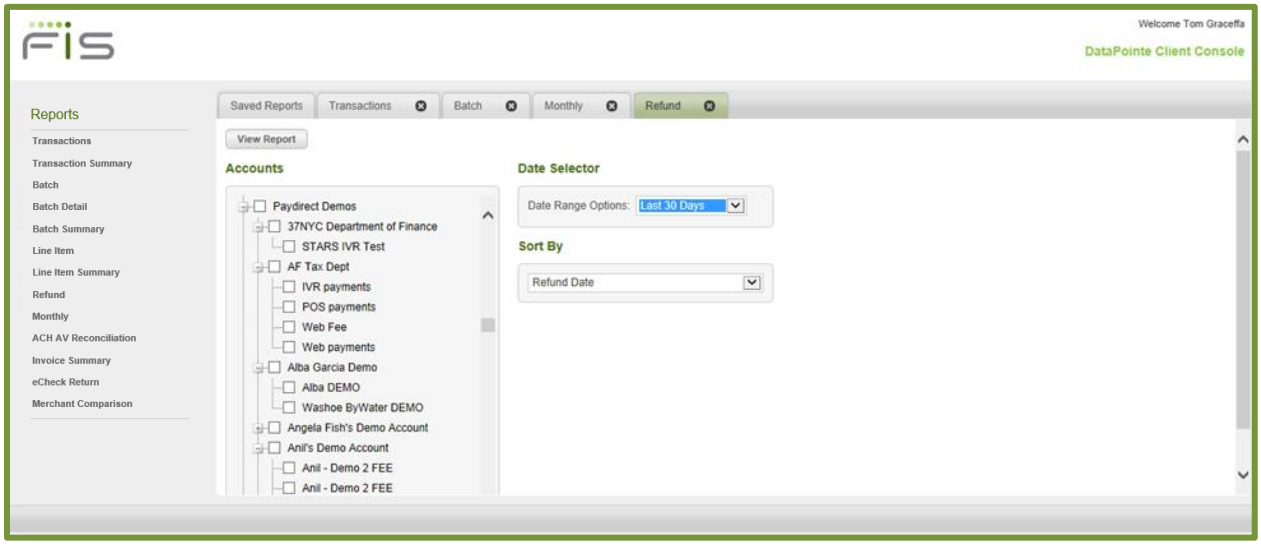
Sample Batch Report



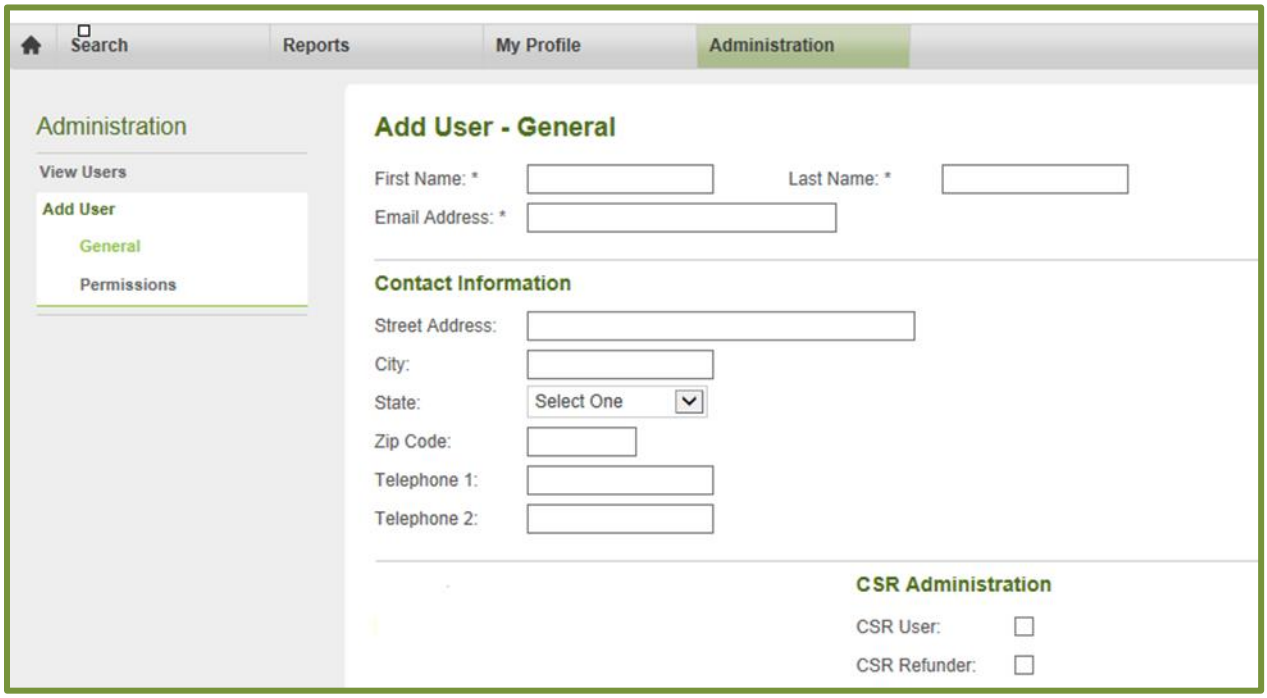
Sample Monthly Summary Report – shows number of transactions broken down by payment method used by end user.



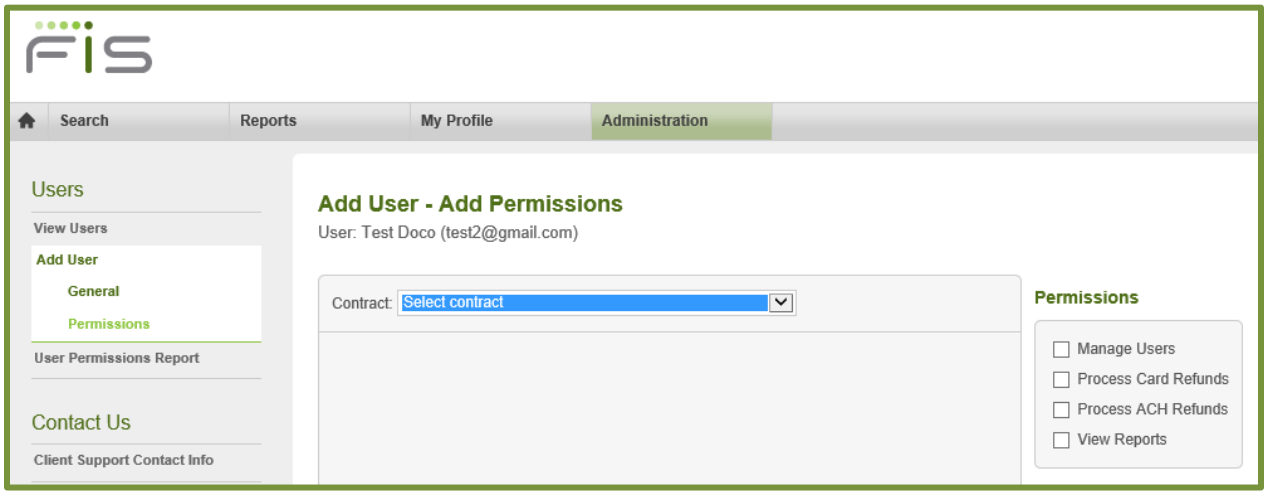
Refund Report Page



Administrator – Add Users



Administrator – Add permissions



Client Support

At FIS, we take pride in providing the highest level of customer support to our clients. As such, we have created two levels of interaction for support, each with their own distinct roles and responsibilities. The team includes Client Support Representatives (Product Support) and Client Services Managers (CSM). Each team is comprised of representatives with extensive working knowledge in both payment processing and our product line to assist our clients throughout the life of the contract.

We embrace a team approach in supporting our clients, therefore there is not a set number of accounts each representative handles. All representatives are available to address your needs, most cases having a first call/first email resolution. The teams report to the Operations Manager. The normal business hours are 7:00am to 7:00pm CST Monday – Friday; however, we provide on-call support for production issues 24/7/365.

Routine Maintenance Schedules

FIS observes routine maintenance windows every Sunday from 12:00 AM - 6:00 AM CST. This is not to say that there is maintenance every weekend, but rather the reservation to utilize this time if needed.

FIS also may observe maintenance windows on Tuesday or Thursday evenings to make updates to the CA testing environment.

Typically, no outage occurs during these maintenance windows. In the event the scheduled maintenance requires an outage, a notice will be provided through a client communication referred to as “Bulletins”. The Bulletin will detail what is being performed and how it may or may not impact your applications.

Contacting FIS

When you contact FIS you will speak to a member of the Product Support team. The Product Support team will work with you to understand the nature of your issue and to triage it, both technical and/or operational.

After gaining the appropriate information, the Product Support team will either resolve your issue on that first call, research it, or route it for further action. That further action could involve more technical research or perhaps support from another entity within our Operations, Development or CSM teams to resolve your issue.

During Normal Business Hours

To provide the best service possible to our clients, FIS suggests the following methods of contact:

- By email during normal business hours
- By phone at our toll-free support line

We strongly recommend contact via phone if you have an urgent production issue to ensure your issue receives immediate attention. In the event the all Support Representatives are busy assisting other clients, your call will be forwarded to the Support voicemail. The voice mail will be reviewed as soon as the Representatives complete the existing calls. Please be sure to leave your name, the client you represent and the call back number to reach you.

Any dissatisfaction with the service received should be escalated to the Director of Operations.

Outside of Normal Business Hours

The Support Team is available to assist you with production related issues outside of normal business hours. They will strive to resolve the issue on the first call or will reach out to the appropriate on-call personnel as needed. If the related issue is occurring in the testing environment or a part of an open project, the request will be relayed to the appropriate teams for research during normal business hours.

Client Services Manager

For inquiries outside of day to day operational items please reach out to our Client Services Managers (CSMs). The CSMs will assist with inquiries relating to contractual items, invoicing, pricing, requests for additional products and services or changes to existing solutions. The CSMs are also available as a point of escalation.

Implementation

Implementation Process

Through extensive experience in project management, FIS has developed the people, procedures, and resources necessary for successful project conversions and implementations. To ensure an efficient and successful implementation for the Client, FIS' Project Management team will employ a step-by-step plan based upon the Project Management Institute's processes and methodologies. This plan includes the following project phases:

Initiation & Planning

The goal of the Project Initiation Phase is to ensure the needs of the Client are adequately articulated so that the Program Manager may formulate the proper goals and objectives of the project. High-level discussions on phase deliverables are conducted during this phase. Additionally, the high-level barriers, potential problems, and roles and responsibilities of the project are summarized. As a result of the Initiation phase, a Scope & Project Management Plan and preliminary project schedule are produced. The Scope & Project Management Plan accurately defines the scope of deliverable, the stakeholders, and roles & responsibilities for project and the project team. It defines how communications will be conducted, how decisions will be made, and how issues, risks, and change will be managed on the project. The project schedule provides a breakdown of the tasks, anticipated deliverables, and significant milestones that are to occur during the project's implementation. These deliverables will be completed both at the Program and at the Project level.

Definition & Design

The Definition Phase involves identifying and documenting how the products to be implemented will be configured to meet the needs of the Client. Once the Client has approved the documented configuration

set for the desired product components, the Project Manager refines the schedule for the remainder of the project.

Execution

During the Execution Phase, the project implements the product components according to the specified configurations. Verification and quality control processes are applied to ensure the completeness and accuracy of the implementation.

Once these implementation tasks are completed, the system is made available to the Client for Client Acceptance (CA) testing. Available 24/7, FIS' CA testing environment is a replica of our production environment. The Client may test all features of the payment solution in CA, with a few minor exceptions related to dependencies on the credit or ACH processor's test system (e.g., money does not actually move). During the CA review, the Client's focus is to test the integration points between the FIS products and external systems in order to validate the configuration choices that were made. Any issues or changes that arise in the CA environment are addressed, allowing the testing to continue. This process continues until the Client is satisfied that the application meets FIS' contractual obligations and the integration with other systems is working as desired. The Client will formally sign-off on the application as configured in CA, and the Project Manager will prepare for deployment to Production.

Closing

The last major phase of a project's life cycle is project closeout. Project closeout is performed once all defined project objectives have been met and the client has accepted the final product. The application is deployed to the live Production environment.

The Project Manager will remain engaged with the client for a Post-Production Monitoring period (typically one-two weeks) to ensure that settlement is occurring as expected and to resolve any remaining issues. At the end of the Post-Production Monitoring period responsibility for the client is transitioned to FIS Customer Service. The project team is released from the project, and the project closes.

Implementation Timeline

During the Program kickoff as well as each individual project kickoff within the Program, FIS will provide a more detailed description of the implementation process, identify stakeholders and project team members. The Program Manager will seek to confirm FIS' understanding of the project scope, goals, and identify major risks, constraints, and assumptions that involve the project. The objective of this first meeting is to enable the creation of a Scope & Project Management Plan and a timeline of milestones (the preliminary schedule).

Communication Tools

FIS uses the following tools to communicate issues and manage a high-quality implementation:

Project Schedule

The project schedule is a document that highlights the tasks required to implement the the client's solution. It identifies respective responsibilities and completion dates for each task. The schedule allows the the client and FIS to monitor the entire process and address related issues. The schedule is an active document and is updated frequently to reflect changing circumstances and implementation progress.

Issues List

The issues list is the primary means of gathering all unplanned items and highlighting those determined to be critical. The application issues are reported on a prioritized basis. This list facilitates the tracking of issues and documents resolutions.

Team Meetings

Regularly scheduled team meetings promote communication and effective review of project plan tasks and issues.

Status Reports

Status reports are provided to the client throughout the project.

Team Members

Implementation Team

Communication between the client and FIS is the key to a successful implementation. As such, we provide a team of qualified experts to assist in the implementation effort. The FIS team is led by an appointed Program Manager who is responsible for the overall management of the implementation process. The FIS team members and their responsibilities are defined as follows:

Project Manager

The Project Manager (PM) has responsibility and accountability for projects and implementations they are managing within the client's Program. This individual directs the effort of the implementation team and ensures that a quality implementation is completed for their project. He is responsible for managing the goals, assessing and managing project risks, and providing feedback to the FIS Program Manager and client stakeholders where appropriate.

Implementation Analysts

The Implementation Analysts will perform all of the technical tasks necessary to complete the project. They assist clients with boarding documentation. They explain how the system can be configured to meet the client's business goals and document the configuration choices that the client makes. Implementation Analysts will implement the product according to the selected configurations and provide the quality control to ensure that the application is correctly implemented. Implementation Analysts will also provide any training required by the client during the project.

Client Stakeholders

Client Stakeholders necessary for project implementation will vary depending upon the choice of products utilized. At times, business stakeholders will be engaged in the planning and training of the products being implemented. This reduces questions once the project goes live, and encourages teamwork between the client and FIS. Stakeholders may also provide project management, business ownership, and customer acceptance testing.

Training

FIS will provide full training services to client personnel as part of the initial project installation. We are committed to providing the highest quality training and education programs in the industry. Well-trained employees of both the client and FIS are vital to the electronic payment solution's success. As such, we will offer thorough education throughout the implementation process and in our continuing education programs.

Since each project is customized to a client's specific needs, we design and develop training on a case-by case basis. Our team has discovered that by working closely with the client throughout the design, development, and implementation of their project, the need for training is significantly reduced. As a result, the training program that we develop will be tailored to the client's particular needs and choice of electronic payment services.

Initial training focuses on utilizing all payment processing equipment and systems, and utilizing administrative site functions, such as our online reporting tool. As new agencies or merchants implement the payment solution, we provide appropriate training to familiarize them with the electronic payment processing services as well.

We have a variety of training methods available:

- On-Site, Instructor-Led Workshops – FIS professionals are well equipped to conduct live training sessions at Client facilities. We will provide all documentation related to training and only require that the client provide workstations with Internet access for demonstrations and hands-on exercises.
- Virtual Training – We utilize virtual training, via the Internet, to deliver many of our training programs, both for converting and existing clients. These virtual training programs, led by a live instructor, provide another efficient option for the client to participate in the training offered by FIS.
- Build Your Own Training Team - Our training professionals can conduct on-site, train-the-trainer sessions to assist the client in building your own training team. Our team can offer advice in creating training programs to complement our systems and fulfill the Client's unique requirements.

Regardless of how the client would like to see your staff trained, FIS is well versed at this task. We are happy to collaborate with the client in developing and implementing a training program that meets the specific needs of your employees. We are committed to providing on-going training and support as necessary.

Security

Security of data is of the utmost importance to FIS. As such, we offer a fully PCI DSS Level I (highest level) audited and compliant electronic payment solution. Our PCI process consists of an annual on-site audit performed by a PCI Security Standards Council (SSC) authorized Quality Security Assessor. This audit includes one week at our location to perform reviews of documentation and systems, as well as interviews with various department heads to ensure that the PCI standards are clearly understood and are being followed at every level within the organization. We also are required to have a PCI SSC authorized Approved Scanning Vendor (ASV) perform quarterly vulnerability scans over the Internet. TrustWave performs an annual on-site review, as well as quarterly unannounced scans. Announced scans are performed monthly by TrustWave TrustKeeper.

In addition, FIS is subject to an annual IRS Security Audit that audits against IRS Publication 4812, NIST, FIPS 140-2, FISMA, and other Federal guidelines such as Executive Orders. These audits include process documentation verification, application scanning, vulnerability scans, penetration testing, network scans, and other intrusive procedures.

We are IRS IV & V certified and our payment system maintains multiple layers of security such as advanced intrusion prevention appliances, event correlation systems, packet filtering firewalls, file monitoring, and denial of service defenses. In addition, we use redundant devices for uptime and security such as firewalls and Application Delivery Controllers. Further, our systems have the ability to use Address Verification Service (AVS), Card Verification Value (CVV2), Card Validation Code (CVC2), Cardholder ID (CID), and Card Security Code (3CSC) to prevent fraud and misuse. These measures are set up during merchant configuration.

To further ensure clients' information is securely transmitted, FIS' systems utilize TLS encryption protocols to ensure that connected clients are indeed on our systems anytime data is transmitted over the Internet. Transaction information is audited, encrypted, and archived in a manner that meets or exceeds the standards defined by PCI, the IRS, and industry best practices.

We employ a role-based security approach by granting access to the data on a need-to-know basis. Access control features of Microsoft Windows Server 2012 and SQL Server 2012 are used to grant access to data and functionality. Within Microsoft Windows Server 2012, developers are restricted to accessing only those administrative tools, utilities, and directories that are essential to their job functions. Limited privilege accounts are established for transferring files from various interfacing

systems/applications. The SQL Server DAC mechanisms are used to define and distinguish access permissions for users and groups within FIS and within the domain. We utilize Secure FTP (SFTP) and TLS Encrypted VPNs in order to exchange sensitive data.

Finally, FIS takes a multi-tiered approach to data security and system integrity in an environment with isolated logical and physical networks. This layered approach relies upon multiple methods to protect the clients' data. FIS utilizes highly advanced security hardware, software and protocols to protect its system including:

- MacAfee SolidCore for an endpoint intrusion detection system, protecting each machine on the network at a device level and monitoring file changes;
- MANDIANT Intelligent Response Agent is installed in all environments/workstations to perform forensic analysis on any system that it is believed could have been breached in order to determine what was accessed;
- SolarWinds and Microsoft Systems Center Operations Manager to monitor system performance and uptime;
- BlueCoat to prevent unauthorized access to the Internet such as social networking sites, external instant messaging (IM), and email;
- BeyondTrust Digital Security Retina for system scanning to detect known PCI and other vulnerabilities related to the operating system and other software installed on the servers;
- BeyondTrust Digital Security Web Reporting (powered by Acunetix) to scan applications written by FIS prior to, and after, deployment into various environments;
- Hewlett-Packard Fortify SSC for static code analysis for detection and remediation of OWASP vulnerabilities;
- Cisco ASA Firewalls are used to segregate internal traffic from Internet traffic via a dedicated DMZ as well as to control access to various internal and external systems and IPs via specific TCP/UDP ports;
- Intrusion Prevention Systems deployed on all networks, logical and physical, and are monitored 24/7 by the FIS Security Incident Response Team (FSIRT) in accordance with FIS Incident Response Plan guidelines; and,

Use of a variety of overlapping monitoring tools so that there is no single reliance upon any single monitoring package and eliminating any single point of failure.

Disaster Recovery (DR)

FIS understands the importance of providing a highly reliable payment solution to your customers while mitigating the risk and liability commonly associated with financial transactions to the client. As such, our solution has multiple layers of redundancy and stability built right in to ensure you and your customers are provided a highly available system. Our fully hosted solution resides on Intel-based Windows servers in a clustered architecture with multi-core processors and site-to-site failover. In addition, our production, testing, and reporting databases reside on separate servers to further speed transactions and increase reliability. FIS' system maintains an availability rate of 99.9 percent 24/7.

Our payment solution features a highly available, horizontally-scaled architecture thereby enabling us to perform most upgrades, maintenance, and fixes without affecting the availability of our services. Our backup systems are geographically dispersed in order to prevent outages due to a catastrophic event. In the highly unlikely event operations are effected by a catastrophic event in our primary site, our services are designed to be restored within 24 hours. We have a DR Plan in place that is tested annually to a backup (standby site) facility to further ensure our systems are continually available for our clients. An overview of our DR plan has been provided below while a full copy can be provided upon request.

DR Plan Overview

Purpose

The increasing dependency on computers and telecommunications for operational support poses the risk that a lengthy loss of these capabilities could seriously affect the overall performance of the organization. A risk analysis has identified several systems as belonging to risk Category I, comprising those functions whose loss could cause a major impact to the organization within 24 hours. It also categorized a majority of business functions as Essential, or Category II – requiring processing support within 72 hours of an outage. This risk assessment process will be repeated on a regular basis to ensure that changes to our processing and environment are reflected in recovery planning.

FIS recognizes the low probability of severe damage to operations, telecommunications, workstation or help desk service capabilities that support the organization. Nevertheless, because of the potential impact to FIS, a plan for reducing the risk of damage from a disaster, however unlikely, is vital. The organization's DR Plan is designed to reduce the risk to an acceptable level by ensuring the restoration of Critical processing within 24 hours, and all essential production (Category II processing) within one week of the outage.

The Plan identifies the critical IT functions of FIS and the resources required to support them. The Plan provides guidelines for ensuring that needed personnel and resources are available for both disaster preparation and response and that the proper steps will be carried out to ensure timely restoration of services.

This DR Plan specifies the responsibilities of the DR Management Team, whose mission is to establish procedures to ensure the continuity of FIS business functions. In the event of a disaster affecting any of the functional areas, the DR Management Teams serve as liaison between the functional area(s) affected and other departments providing major services. These services include the support provided by Facilities and Security.

Assumptions

The Plan is predicated on the validity of the following assumptions:

The situation that causes the disaster is localized to Systems and/or Operations supporting a functional IT area, the building or space housing a functional IT area, or to the telecommunication systems and networks that support a functional IT area.

It should be noted however, that the Plan would still be functional and effective even in an area-wide disaster. Even though the basic priorities for restoration of essential services to the IT Operations organization will normally take precedence over the recovery of an individual department, the FIS IT DR Plan can still provide for a more expeditious restoration of our resources for supporting key functions.

The Plan is based on the availability of the hot sites or the backup resources. The accessibility of these, or equivalent backup resources, is a critical requirement.

The Plan is a document that reflects the changing environment and requirements of FIS Operations. Therefore, the Plan requires the continued allocation of resources to maintain it and to keep it in a constant state of readiness.

Testing

Testing the DR Plan is an essential element of preparedness. Partial tests of individual components and recovery plans of specific functional areas within IT Operations will be carried out on a regular basis. A comprehensive exercise of our continuity capabilities and support by our designated recovery facilities will be performed on an annual basis.

Competitive Advantage

FIS' payment industry expertise, combined with our ability to offer multiple applications, services, and integrated solutions to our clients enhances our competitiveness against companies with more limited offerings. We are a single source provider of a broad range of payment services allowing our clients to service the needs of their customers.

Our competitive factors include:

- FIS ranked first in the 2017 IDC FinTech Rankings. These rankings, by American Banker, Bank Technology News and research firm IDC Financial Insights, are solely based on the percentage of 2016 company revenues derived from the financial services industry.
- One of only three certified payment providers for the IRS
- Delivers comprehensive solutions to more markets in more industries in more countries than anyone else in the world
- Global company with over 55,000 employees and over 130 locations worldwide
- Owns and operates the NYCE EFT/PIN-debit network
- PCI DSS Level I audited and compliant
- Dedicated business unit for federal, state, and local government agency payments
- Single lump sum settlement – one deposit for all payment types
- Consolidated settlement by application, card type, or payment channel for easier reconciliation
- Comprehensive, online reporting in real-time
- Payment remittance file for importing payments instead of hand keying
- 24/7 support
- Lower implementation costs
- Ease of integration